ABSTRACT

A method and system are described to allow the encryption and decryption of a plaintext string of symbols, e.g. a paragraph of English text, using a key consisting in part of an executable computer program. The method and system is such that an attacker who seeks to recover the plaintext from the ciphertext, without knowing the key, can produce a very large number of decrypt attempts that are plausible, but unrelated in meaning to the original plaintext. However the attacker cannot know whether any one of the attempted decrypts is the correct original plaintext. A property of the method and system is that, if the same plaintext is encrypted twice using the same key, the respective ciphertexts are normally different, and normally have different lengths.